IT Contingency Plan Checklist

This document is intended to assist SSOs and contractors assess existing IT contingency plans and determine its compliance with the Department's IT Contingency Planning Guide version 4.0.

Department IT Contingency Plan/DRP Requirements

1. All FSA General Support Systems and Major Applications must create and maintain an IT Contingency Plan (also synonymously called Continuity of Support Plan) and a Disaster Recovery Plan.
2. Tier 1 and Tier 2 systems require describing only Continuity of Support functions in the Contingency Plan. Tier 3 and 4 systems require descriptions of Continuity of Support and a Disaster Recovery Plan. The Department's Certification and Accreditation Guide explains the criteria for the Tier ranking

Quick list of frequently asked questions:

1. Q: *What is the difference between a Disaster Recovery Plan, a Continuity of Support Plan, and an IT Contingency Plan?*
   A: The DRP applies to major, usually catastrophic, events that deny access to the normal facility for an extended period. The DRP refers to an IT-focused plan designed to restore operability of the target system, application, or computer facility at an alternate site after an emergency. The DRP scope may overlap that of a Continuity of Support Plan; however, the DRP is focused on long-term outages (over 48 hours) that require relocation to an alternate processing site. The DRP does not address minor disruptions that do not require relocation. Continuity of Support Plans are intended to provide guidance for short-term service interruptions (less than 48 hours) that do not require relocation to an alternate processing site. (From ED guide). The IT Contingency Plan is not an actual documented plan, but rather a term used to describe the overall contingency planning process.
2. Q: *When do I use my Continuity of Support Plan and when do I use my Disaster Recovery Plan?*
   A: The Department states that the Continuity of Support plan is used during short-term interruptions, lasting less than 48 hours, and do not require relocation to an alternate site.
3. Q: *How does an MA's Contingency Plan relate to its GSS's Contingency Plan?*
   A: Tough question. Some FSA systems rely on the VDC as its only GSS, but many other FSA systems rely on the VDC, EDNet, SAIG, and other operating facilities across the country. Major applications have two primary roles in Contingency Plan development: communication strategy and application recovery.

   The communication strategy establishes who the decision makers are after an event, determines the order of notification once an event has occurred (call tree), and defines what information needs to be provided to each person on the call tree. The key is to develop clear lines of communication between the GSS and the MA.

   Because the GSS generally does not administer the application, the recovery of the application is another responsibility of the MA team. At the very least, the MA team must develop contingency procedures for recovering the application. Even though

personnel employed by the GSS may physically restore the system, the MA owner must give procedures to the GSS personnel to carry out the application's recovery actions.

Enough with the definitions. Let's get to the IT Contingency Plan Assessment. First, you need to answer two basic questions below.

Is your system a GSS/MA/A?	
What tier level are you?	

IT Contingency Plan Assessment

Forming the Contingency Plan	Completed	Not completed, Justification
3.2 - Did someone conduct a Business Impact Analysis for your system?		
3.2.1 - During the BIA, were essential IT resources identified?		
3.2.1 - Were system interdependencies determined?		
3.2.1 - Are clear responsibilities for the GSS and MA delineated in the plan?		
3.2.2 - During the BIA, did someone determine the system impact if a resource was lost for various lengths of time?		
3.2.2 - Were cascading effects determined; that is, if one system or system component went down, how would its loss affect other systems?		
3.2.2 - Was the time of year taken into consideration when determining the impact of the outage?		
3.2.3 - Were recovery priorities created based on their allowable outage times and effects across related systems?		
3.3 – Were preventive measures/security controls identified that will reduce the impact of an outage?		
3.4 - Is a recovery strategy articulated in the plan?		
3.4 - Does the recovery strategy consider data backup, recovery site, and equipment replacement needs?		
3.4.1 - Does the backup policy include backup frequency, backup storage time frame and details on the off-site storage location?		
3.4.2 - For tier 3 and 4 systems, does the plan identify an alternate processing site?		

3.4.2 - Does the plan identify if the alternate site is a cold, warm, hot, mobile, or mirrored site and why that type of site was chosen?		
3.4.3 - If equipment at the primary site is destroyed or becomes inoperable, does the plan describe how new equipment will be procured?		
3.4.3 - Does an agreement exist that describes any contractual agreements to replace inoperable equipment during an outage?		
3.4.3 - If the GSS or MA uses a backup facility for recovery purposes, is there an agreement establishing recovery priorities (including priorities with other non-FSA systems also hosted at the backup facility)?		

3.6 - Is a Contingency Plan test strategy described in the plan?		
3.6 – Is the plan tested on a regular basis?		
3.6.1 - Does the Contingency Plan test strategy contain information for conducting the test, guidelines for when the test will be run and under what conditions, what are the tests success measures, and how weaknesses will be documented and reported?		
3.6.1 – Are Contingency Plan tests based upon specific, measurable test objectives?		
3.6.1 – Are detailed test procedures created, delineating when the test will be run, under what conditions, and how any weaknesses/deficiencies will be reported to management?		
3.6.1 – Is a walk-through of the test plan conducted before running the test?		
3.6.1 – After completing the test, are any identified weaknesses documented and reported to the system's management?		
3.6.1 – After identified weaknesses have been corrected, is the system tested again, focusing primarily on the changes made after the first test?		

3.7 Are maintenance measures identified for the IT Contingency Plan?		
3.7 - Does the plan contain plan maintenance guidelines?		
3.7.1 - Are version control and plan distribution procedures identified in the plan?		

Implementing the IT Contingency Plan -	Completed	Not completed, Justification
4.2.1 – Does your IT Contingency Plan contain procedures for notifying recovery personnel once an event has occurred?		
4.2.2 – Is a team identified to assess the damage of an event and provide a plan activation recommendation to the Contingency lead?		
4.2.3 – Does your IT Contingency Plan contain procedures for activating the plan?		
4.3 – Does your IT Contingency plan establish recovery procedures to make the system operational after an event?		
4.4 – Does your IT Contingency plan contain detailed descriptions and easy-to-follow procedures for system reconstitution?		

IT Contingency Plan Artifacts	Completed	Not completed, Justification
Does your IT Contingency Plan have the following information in the plan or in referenced appendices?		
Contact information for staff and vendors		
Alternate site information		
Business impact analysis documentation		
List of Acronyms		

Roles and Responsibilities	Team Lead	Alternate
Who (if applicable) has been assigned as the team lead and alternate team lead for the following Contingency Plan subteams? (indicates mandatory subteam)*		
Management *		
GSS/MA Coordination		
Damage Assessment		
Server Recovery		
Application Recovery		
Database Recovery		
Alternate Site Recovery		
Media Relations		
Legal Affairs		
Physical/Personnel Security		

Testing/Training	Completed	Not completed, Justification
3.6 - Is the contingency plan tested and are associated personnel trained in their roles?		
3.6 – Are personnel (including contractors) with roles in the system's recovery and continuity provided training in their Contingency Plan roles?		

3.6.2 – Are personnel trained at least annually in their roles in the Contingency plan?		
3.6.2 – Are new hires with contingency plan responsibilities trained immediately after starting employment?		
3.6.2 – Are team members trained to be familiar enough with their roles and responsibilities to execute them without the aid of the written contingency plan?		
3.6.2 – Are the following elements covered in training:		
▪ Purpose of the plan?		
▪ Cross-team coordination and communication?		
▪ Reporting procedures?		
▪ Security requirements?		
▪ Team specific processes during the activation/notification, recovery, and reconstitution phases?		
▪ Individual responsibilities during the activation/notification, recovery, and reconstitution phases?		